Název veřejné zakázky: **KYBEZ města Litvínov - Audit kybernetické bezpečnosti; §16 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti**

systémové číslo: P25V00000093

# Předmět veřejné zakázky

**Nejedná se o audit celé organizace Zadavatele.**

Předmětem veřejné zakázky je provedení nezávislého auditu kybernetické bezpečnosti, který ověří implementaci opatření kybernetické bezpečnosti zavedených v rámci projektu Kybernetická bezpečnost města Litvínov (registrační číslo CZ.31.2.0/0.0/0.0/23\_093/0008361) podpořeného z programu Národní plán obnovy (NPO), komponenta 1.2 Digitální systémy veřejné správy.

Audit je nezbytný pro doložení splnění monitorovacích indikátorů projektu, zejména potvrzení úspěšného posílení kybernetické bezpečnosti klíčových informačních systémů.

# Soulad auditu

Audit musí být proveden v souladu:

* se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, a jeho prováděcími předpisy, včetně vyhlášky č. 82/2018 Sb.;
* s požadavky výzvy č. 41 verze 3 – Kybernetická bezpečnost – obce;
* s Pokyny vlastníka komponent 1.1, 1.2, a 4.4 pro příjemce finanční podpory, v platném znění;
* s FAQ Ministerstva vnitra České republiky k výzvám v oblasti zajištění kybernetické bezpečnosti.

# Požadavky auditora

Audit musí provádět auditor, který splňuje požadavky dle odst. 5.4, písm. b) Zadávací dokumentace.

# Rozsah a cíl auditu

Cílem finálního auditu je porovnání projektové dokumentace žadatele na vstupu (Popis výchozího stavu, produkty / podprodukty v právním aktu projektu) s výstupy projektu (výsledný stav realizace, tzn. co bylo definováno, bylo pořízeno, implementováno, je funkční) a posouzení, zda realizace projektu přispěla ke zvýšení kybernetické bezpečnosti žadatelem definovaných informačních systémů. Auditor ve svém znaleckém posudku v zásadě odpoví na dvě otázky:

1. Došlo k nasazení vybraných technologií či služeb dle předloženého projektu?
2. Došlo u vybraných informačních systémů, které jsou předmětem projektu, prostřednictvím realizace zvolených opatření k posílení jejich kybernetické bezpečnosti?

# Posilované informační systémy

Audit KB bude ověřovat posílení IS:

* Gordic GINIS – páteřní IS úřadu, ve kterém se vede spisová služba, účetnictví, ekonomika, majetek, daně, dávky, poplatky, pohledávky
* VITA – druhý nejvýznamnější IS úřadu, ve kterém se vede kompletní agenda stavebního úřadu a veškeré typy přestupků
* FLUX – IS ve kterém se vedou mzdy a personalistika
* PowerKey – IS ve kterém se vede docházka a přístupová oprávnění do budov
* Marbes EOS – identitní systém
* Microsoft ActiveDirectory – adresářová služba uživatelských účtů a oprávnění
* Microsoft SQL – databázový systém, ve kterém jsou vedeny databáze všech IS
* Microsoft Exchange – on premise poštovní server
* ArcGIS – IS, ve kterém se vedou digitální pasporty úřadu PWS Plus VOX – varovný systém města iQ Metropolis – komplexní IS pro potřeby výkonu Městské policie

# Zaváděná opatření

Audit KB bude ověřovat zavedená opatření:

* § 19 - Centrální systém pro ověřování uživatelů a správu, monitoring aktivních prvků - Zajištění ochrany sítě bude zajištěno a doplněno o software řešení pro řízení přístupu uživatelů a zařízení do drátové i bezdrátové LAN sítě se sadou pokročilých funkcionalit zefektivňujících procesy s tímto spojené. Detailně viz Studie proveditelnosti.
* § 20 - Rozšíření IDM EOS - Realizací opatření dojde k rozšíření IDM EOS o další moduly, které umožní komplexní řízení práv a přístupů k aplikacím na úřadu a významně posílí kybernetickou bezpečnost v oblasti chování uživatelů. Detailně viz Studie proveditelnosti.
* § 24 - Centrální sběr logů - V rámci opatření bude pořízen Log Manager, který zajistí jednotné úložiště logů, sběr logů do tohoto úložiště v reálném čase, analýzu logů v reálném čase a operativní práci v reálném čase. Detailně viz Studie proveditelnosti.
* § 25 – DLP – Realizace opatření umožní monitorovat data na koncových stanicích a rovněž na serverech, a to i při jejich přenosu po síti. Díky tomu bude možné efektivně zabránit úniku či ztrátě dat, ať již například přes externí média, jakými jsou flash-disky, USB, externí disky atp., tak i při odeslání dat elektronickou poštou, jejich sdílením do webové sítě či vytisknutím. Detailně viz Studie proveditelnosti.
* § 25 - Systém zabezpečení a správy koncových stanic - Systém zvýší bezpečnost koncových stanic integrací např. s Firewally, integrací do VPN klientů, možností zavedení dvoufaktorového ověřování apod. Detailně viz Studie proveditelnosti.
* § 25 - Řízení aktiv a konfigurační databáze - Opatření zajistí kompletní evidenci seznamu vedených aktiv včetně jejich lokalizaci a dále zajištění konfigurační databáze vedených aktiv včetně vedení provazeb mezi jednotlivými aktivy. Dále napojení tohoto nástroje a naplnění nástroje daty o vedených aktivech – vytvoření CMDB, která bude dále udržována pracovníky města. Detailně viz Studie proveditelnosti.
* § 25 – RDS - V rámci projektu bude implementováno řešení s možností centrální správy, bezpečné doručování aplikací pomocí zabezpečeného spojení HTTPS, chráněného případně dvoufaktorovým ověřováním. Opatření umožní virtualizaci jak aplikací, tak celých pracovních uživatelských prostředí. Detailně viz Studie proveditelnosti.
* § 27 - Redundantní infrastruktura - Realizace opatření spočívá ve vybudování redundantní infrastruktury, která bude sloužit jako záložní pro provedení obnovy uložených záloh. Eliminuje se tak riziko pozastavení chodu úřadu z důvodu nefunkčnosti / nedostupnosti dat a informací.

# Závěrečná zpráva

Na základě provedeného auditu bude připravena komplexní závěrečná zpráva, která shrne klíčová zjištění a vyhodnotí soulad či nesoulad dle kritérií dotační výzvy. Součástí zprávy bude také posudek auditora, který odpoví na klíčové otázky týkající se realizace opatření a jejich dopadu na kybernetickou bezpečnost.